Vers une synthèse d'arbres d'attaque pour une analyse de risques assistée par ordinateur

Stéphanie Georges, Sophie Pinchinat

Vers une synthèse d'arbres d'attaque pour une analyse de risques assistée par ordinateur

Stéphanie GEORGES [1], **Sophie PINCHINAT** [2]

IRISA, Université de Rennes 1
35042 RENNES
FRANCE
{stephanie.georges,sophie.pinchinat}@irisa.fr

RÉSUMÉ. *L'analyse de risques est une discipline consistant à identifier et à évaluer les risques qui menacent un système donné afin de les atténuer ou de les éliminer grâce à l'application de protocoles de sécurité (gestion de risques). Après (Bornette* et al.*, 2005), nous avons développé une méthode ayant pour but de construire de façon automatique des scénarios d'attaque contre un système à protéger. Elle consiste principalement en l'extraction de ces scénarios, exprimés sous la forme de suites d'actions élémentaires permettant d'atteindre, à partir d'un état initial, un objectif donné (exprimé sous la forme d'un ensemble de dommages à causer au système), du graphe représentant le système. Grâce à l'utilisation d'une grammaire d'actions, nous en déduisons un arbre d'attaque mettant en évidence les failles du système étudié. Cette méthode doit aboutir à la conception d'un outil à destination des experts. Il ne leur reste alors qu'à déterminer des contremesures empêchant la réalisation effective de ses attaques.*

ABSTRACT. *Risk Analysis is a discipline consisting in identifying and evaluating risks that threaten a given system in order to reduce or annihilate them by defining actions to engage (risk management). After (Bornette* et al.*, 2005), we have developed a method aiming at building attack scenarios against a system that has to be protected. We describe this method in the present article. The main principle is to extract from a dedicated model of the system the scenarios (expressed as a succession of elementary actions) allowing to reach, from an initial state, a given goal (expressed as a set of damages against which we want to provide countermeasures). Thanks to the use of high-level actions, these scenarios are then gathered into an attack tree allowing after specific processing to highlight flaws to bring down.*

MOTS-CLÉS : *analyse de risques, arbre d'attaque, graphe d'attaque, hiérarchie d'actions, sécurité des systèmes.*

KEYWORDS: *attack graph, attack tree, hierarchy of actions, risk analysis, system security.*

1. Introduction

Assurer la sécurité d'un système d'information signifie garantir la disponibilité, l'intégrité et la confidentialité de ses données. Pour atteindre cet objectif, une étude préliminaire, appelée analyse de risques, du système et de son environnement est nécessaire. Beaucoup de méthodes se limitent à la recherche de dangers liés à l'informatique pure et négligent les menaces qui pèsent sur les locaux qui abritent les systèmes à protéger. Il est évident que les meilleures mesures de protection logique seront inefficaces contre une destruction physique de matériel. Pour cette raison ainsi que pour une compréhension plus aisée des points théoriques abordés, nous nous sommes concentrés à travers un exemple simple sur cet aspect (physique) de la sécurité de l'information.

2. La méthode proposée

Comme on peut le voir dans (Bursztein, 2008), les méthodes actuelles suivent, pour la plupart, la même structure : décomposition du système en sous-systèmes, production d'un modèle, établissement d'une liste d'évènements redoutés et caractérisation des raisons potentielles de la réalisation de ces évènements. Jusqu'à maintenant, ces étapes se font "à la main", et sont basées sur les connaissances et l'expérience des analystes et techniciens. Notre but est de créer un processus automatisé d'assistance à la réalisation de ces tâches. La méthodologie que nous proposons repose sur le concept de (Bornette *et al.*, 2010) : il s'agit de se placer du point de vue de l'attaquant et de chercher à atteindre un état de vulnérabilité du système. Cette méthodologie est la suivante :

1. Décrire le système à protéger sous la forme d'un graphe d'attaque,
2. Extraire les attaques,
3. Rassembler les attaques dans un arbre d'attaque.

La première étape consiste à modéliser le système et ses fonctionnalités, de façon similaire à (O. M. Sheyner, 2004) ou (Mehta *et al.*, 2006). C'est un point essentiel car la complétude de la représentation assure que les traitements permettront de produire l'ensemble des attaques souhaitées. Nous avons choisi le graphe d'attaque, structure obtenue par la combinaison d'états de modules (composés d'un ensemble de variables et d'actions pouvant agir sur ces variables) représentant les sous-systèmes. La deuxième étape est un problème de planification : en effet, il s'agit de trouver les chemins dans le graphe qui respectent certaines conditions, à savoir atteindre un état du système le rendant vulnérable, appelé état-but, à partir d'un état dans lequel le système est "à l'équilibre", dans un état de fonctionnement habituel, dit état initial.

Ces deux premières étapes ont été longuement étudiées par (O. Sheyner *et al.*, 2002) dans le domaine des réseaux informatiques, qui propose déjà un algorithme pour la génération automatique de graphe d'attaque et qui résume les menaces dans un graphe de scénarios.

Enfin, la troisième étape peut être réalisée grâce à la connaissance existante (antérieure) du système amenant à spécifier des actions de haut niveau (voir (Marthi *et al.*, 2007)), permettant ensuite d'abstraire certaines séquences d'actions. On en déduit une hiérarchie d'actions que l'on relie de façon naturelle à une grammaire algébrique. On recourt alors à l'analyse syntaxique pour construire une stratégie, objet (forêt d'arbres) décrivant tous les niveaux d'abstraction possibles pour chaque attaque. Une fois obtenues, ces stratégies sont regroupées dans un *arbre et/ou* : l'arbre d'attaque (objet formalisé par (Mauw, Oostdijk, 2005) qui permet d'évaluer le risque réel pesant sur un système (Edge *et al.*, 2006)).

3. Conclusion

L'approche proposée ici –construction d'un graphe d'attaque représentant le système, extraction des attaques pertinentes, génération de l'arbre d'attaque associé– nécessite des recherches supplémentaires afin d'établir plus précisément son niveau de complexité et identifier les principaux verrous technologiques. En effet, le nombre d'états contenus dans le graphe d'attaque risque de croître de façon exponentielle avec le nombre de sous-systèmes étudiés. L'exemple pris dans notre article long décrit un simple bureau renfermant un coffre-fort. Nous avons dépeint ce système à l'aide de trois variables binaires, soit 2^3 états. Or, dans le domaine de la sécurité physique, nous avons besoin de pouvoir détailler tout un bâtiment et ses sous-systèmes. L'outil que nous aimerions développer devra donc s'appuyer sur des moyens très efficaces permettant notamment d'éviter une potentielle explosion du nombre d'états dans les représentations des gros systèmes ou d'y rechercher en un temps "raisonnable" un ensemble de chemins, comme, par exemple, la description symbolique du système associée à des techniques de model-checking. L'outil devra aussi offrir un environnement ergonomique pour les utilisateurs. La méthode développée vise à être outillée pour automatiser l'étude de systèmes. Il s'agit d'une étape importante à la contribution technique que nous voulons apporter dans ce domaine de l'analyse de risques. Cela faciliterait en effet le travail de l'analyste qui gagnerait alors en temps et en fiabilité de résultats. Nous projetons d'automatiser également l'étape suivante de l'analyse, à savoir la caractérisation des scénarios (valuation des différents critères de tri choisis par les experts, comme le temps de réalisation du scénario, son coût financier,...) et leur tri.

Bibliographie

Bornette E., Lebée J.-P., Eymery D. (2005). Nouvelle approche méthodologique de l'analyse de risques reposant sur le point de vue de l'attaquant.

Bornette E., Lebée J.-P., Eymery D. (2010). Nouvelle approche méthodologique de l'analyse de risques reposant sur le point de vue de l'attaquant. In *Proceedings of of the 5th conference on network and information systems security (sar/ssi 2010), rocquebrune cap-martin, france.*

Bursztein E. (2008). *Anticipation games - théorie des jeux appliquée à la sécurité réseau*. Thèse de doctorat non publiée, ENS Cachan.

Edge K. S., II G. C. D., Raines R. A., Mills R. A. (2006). Using Attack and Protection Trees to Analyze Threats and Defenses to Homeland Security. In *Proceedings of the 2006 ieee conference on military communications*, p. 953–959. IEEE press.

Marthi B., Russell S., Wolfe J. (2007). *Angelic Semantics for High-Level Actions*. Rapport technique. EECS Departement, University of California, Berkeley.

Mauw S., Oostdijk M. (2005). Foundations of Attack Trees. In *International conference on information security and cryptology - icisc 2005. lncs 3935*, p. 186–198. Springer.

Mehta V., Bartzis C., Zhu H., Clarke E., Wing J. (2006). Ranking Attack Graphs. In *Proceedings of recent advances in intrusion detection.*

Sheyner O., Haines J., Jha S., Lippman R., Wing J. (2002). Automated Generation and Analysis of Attack Graphs. In *Proceedings of the 2002 ieee symposium on security and privacy*, p. 273–. IEEE Computer Society.

Sheyner O. M. (2004). *Scenario Graphs and Attack Graphs*. Thèse de doctorat non publiée, University of Wisconsin.